



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,231	06/12/2001	Ron Karim	15437-0508	5058

29989 7590 02/11/2005

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER

WU, QING YUAN

ART UNIT PAPER NUMBER

2126

DATE MAILED: 02/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/880,231

Applicant(s)

KARIM, RON

Examiner

Qing-Yuan Wu

Art Unit

2126

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

1. Claims 1-36 are pending in this application.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schnurer et al (hereafter Schnurer) (U.S. Patent 5,842,002).

4. Schnurer was cited in the last office action.

5. As to claim 1, Schnurer teaches the invention substantially as claimed including a computer-implemented method for executing an untrusted program [abstract, lines 1-2], comprising:

establishing a limited environment within a general environment [col. 6, lines 56-58; Fig. 3 and 4], said limited environment comprising at least one mock resource [col. 4, lines 16-20, 22-26, 47-49; col. 7, lines 3-8]; general environment comprises at least one real resource [col. 4, lines 24-25]

executing at least a portion of an untrusted program within said limited environment [col.7, lines 5-12]; and examining said limited environment after execution of at least said portion of said untrusted program to check for undesirable behavior exhibited by said untrusted program [col. 4, lines 32-36; col. 7, lines 12-15; 48, 50, 52, Fig. 1].

6. Schnurer does not specifically teach wherein said limited environment and said general environment are both implemented using the same type of operating system. However, Schnurer disclosed that his invention could be done without a transplatform, or the use of a foreign operating system [col. 4, line 63-col. 5, line 4], if safety and speed are not the concern.

7. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have recognized that even though the implementation of Schnurer's invention using the same operating system it is not recommended, it could be done.

8. As to claim 2, Schnurer teaches the invention substantially as claimed including where said limited environment precludes access to actual resources, which if altered or accessed by said untrusted program, may lead to undesirable consequences [abstract; col. 5, lines 5-10; col. 7, lines 15-18].

9. As to claim 3, Schnurer does not specifically teach a limited environment comprises a shell in a UNIX operating system environment. However, Schnurer disclosed different operating

systems [col. 3, lines 59-66]. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to have included a UNIX operating system in Schnurer et al's system because UNIX is well known to be a powerful operating system.

10. As to claim 4, Schnurer teaches the invention substantially as claimed including wherein examining said mock environment comprises: determining whether said mock resource has been deleted [col. 4, lines 37-39; col. 7, lines 12-15].

11. As to claims 5-6, and 9, Schnurer teaches the invention substantially as claimed in claim 1. Schnurer does not specifically teach the step of determining whether said mock resource has been renamed, moved and last updated. However, Schnurer disclosed that his system could detect any malicious act by the virus, including the activities of changing the FAT table and changing of the error checking algorithm [col. 7, lines 59-60; col. 8, lines 25-26; col. 4, lines 37-39].

12. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have recognized that common viral activities or critical behaviors exhibited by viruses would have included the renaming, moving, and updating of system resources as being considered and implemented in Schnurer et al's method of virus detection.

13. As to claim 7, Schnurer teaches the invention substantially as claimed including wherein examining said mock environment comprises: determining whether said mock resource has been altered [col. 7, line 48 to col. 8, line 26].

14. As to claim 8, Schnurer teaches the invention substantially as claimed including wherein said mock resource has a parameter associated therewith which changes when said mock resource is altered, and wherein determining whether said mock resource has been altered, comprises:

determining whether said parameter has changed [col. 7, line 48 to col. 8, line 26].

15. As to claim 10, Schnurer teaches the invention substantially as claimed including wherein examining said mock environment comprises:

determining whether said mock resource has been accessed [col. 7, line 48 to col. 8, line 26].

16. As to claim 11, Schnurer does not specifically teach wherein said mock resource contains one or more sets of content, and searching a particular portion of memory for at least one of said one or more sets of content. It is well known in the art that when a file gets accessed or altered, traces of the contents being accessed is located in the memory, in addition, Schnurer disclosed the determination of potential viral activities by examining “if anything within the environment changes...” [col. 7, line 48 to col. 8, line 26].

17. As to claim 12, Schnurer teaches the invention substantially as claimed including providing information indicating behavior exhibited by said untrusted program [col. 7, line 25 to col. 8, line 26].

18. As to claims 13 and 14, Schnurer teaches the invention substantially as claimed including wherein said information comprises indications of undesirable behavior exhibited by said untrusted program [col. 7, lines 48-52], and in response to a determination that said untrusted program has exhibited undesirable behavior, taking corrective action [col. 8, lines 27-35; 52, Fig. 1].

19. As to claims 15 and 16, Schnurer teaches the invention substantially as claimed including wherein taking corrective action comprises: deleting said untrusted program and warning to a user [col. 8, lines 27-35; 52, Fig. 1].

20. As to claim 33, Schnurer does not specifically teach wherein said limited environment and said general environment are both implemented on the same machine. However, Schnurer disclosed trapping device within a network environment [col. 6, lines 56-58; Fig. 3 and 4]

21. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have modified the teaching of Schnurer by implementing the limited environment in the same machine as the general environment if the limited environment is limited to protect a specific machine.

22. As to claim 35, this claim is rejected for the same reason as claims 1, and 33 above.

23. As to claims 17-32, 34, and 36 these are system claims that correspond to the method claims 1-16, 33, and 35. Therefore, they are rejected for the same reason as claims 1-16, 33, and 35 above.

Response to Arguments

24. Applicant's arguments with respect to claims 1-32 have been considered but are moot in view of the new ground(s) of rejection.

25. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Qing-Yuan Wu whose telephone number is (571) 272-3776. The examiner can normally be reached on 8:30am-5:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Qing-Yuan Wu

Examiner

Art Unit 2126


MENG-AI T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100